(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－232487
（P2002－232487A）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	12/58	100	H04L 12/58	100Z	5B089
G06F	13/00	351	G06F 13/00	351Z	5J104
		610		610S	5K030
G09C	1/00	640	G09C 1/00	640B	
H04L	12/66		H04L 12/66	E	

審査請求　未請求　請求項の数11　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－25758(P2001－25758)

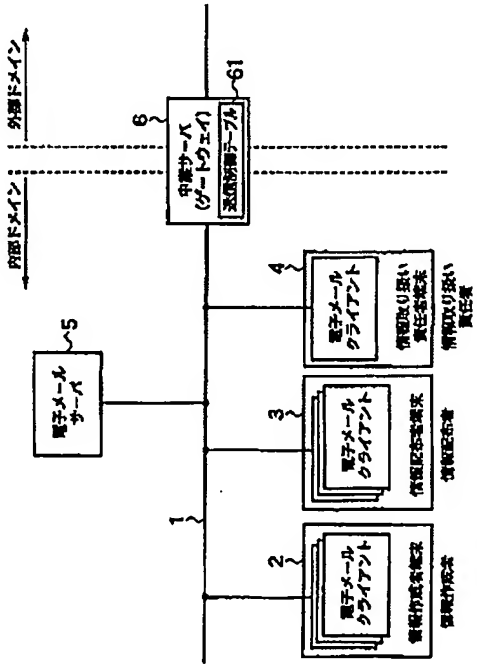
(22)出願日　平成13年２月１日(2001.2.1)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　高橋　陽一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝小向工場内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

Ｆターム(参考)　5B089 GA31 GB02 JA31 KA17 KB13 KC52 KC54 LA01
5J104 AA09 LA03 LA05 LA06 NA02 PA08
5K030 GA15 HA08 HC01 HC14 JA11 LD20

(54)【発明の名称】　電子メールシステム及び電子メール送信制御方法並びに中継装置

(57)【要約】
【課題】　証明書と署名により電子メールの送信の厳密性を保証し、証明書の判定の厳密性を変えることにより、ポリシーに応じて使いやすさと安全性程度を選択できる電子メールシステムを提供する。
【解決手段】　電子メールサーバ５が端末２，３，４から電子メールを受信し、中継サーバ６が電子メールサーバから電子メールを受信し、基本設定として外部ドメインへの電子メールの送信を禁止し、特定の条件が成立した場合に外部ドメインへの電子メールの送信を許可する。また、端末は、添付ファイルを作成する際に添付ファイルの内容を証明するファイル証明書を作成し、ファイル証明書に署名することにより添付ファイルとファイル証明書との関係及び内容を保証し、中継サーバは、端末から送られてくる添付ファイルに付加されたファイル証明書及び署名の内容に基づいて外部ドメインへの電子メールの送信可否を決定し、許可された内容の電子メールのみを外部ドメインに送信する。



1

【特許請求の範囲】

【請求項１】　外部ドメインとの間で電子メールを送受信する電子メールシステムにおいて、

電子メールを送受信する端末と、

この端末からネットワークを介して電子メールを受信し、基本設定として前記外部ドメインへの前記電子メールの送信を禁止し、特定の条件が成立した場合に前記外部ドメインへの前記電子メールの送信を許可する中継サーバと、を備えることを特徴とする電子メールシステム。

【請求項２】　前記端末において、添付ファイルを作成する際に、この添付ファイルの内容を証明するファイル証明書を作成し、このファイル証明書に署名することにより添付ファイルとファイル証明書との関係及び内容を保証し、

前記中継サーバは、前記端末から送られてくる前記添付ファイルに付加された前記ファイル証明書及び署名の内容に基づいて前記外部ドメインへの前記電子メールの送信可否を決定し、許可された内容の電子メールのみを前記外部ドメインに送信することを特徴とする請求項１記載の電子メールシステム。

【請求項３】　前記端末において、電子メールを送信する際に、電子メールの配布先及び配布内容を記載した配布リストを作成し、この配布リストに署名することにより電子メール本体と配布リストとの関係及び内容を保証し、

前記中継サーバは、前記端末から送られてくる前記電子メールに付加された前記配布リスト及び署名の内容に基づいて前記外部ドメインへの前記電子メールの送信可否を決定し、許可された内容の電子メールのみを前記外部ドメインに送信することを特徴とする請求項１又は請求項２記載の電子メールシステム。

【請求項４】　前記端末において、前記配布リストにより配布リストと電子メール本体と前記添付ファイルとの関係を保証し、前記ファイル証明書により前記添付ファイルと前記ファイル証明書との関係を保証し、前記配布リストと前記ファイル証明書との関係を前記添付ファイルを介して間接的に保証することにより、必要に応じて前記添付ファイル証明書又は前記配布リストを削除しても個々の保証関係に問題を生じないことを特徴とする請求項３記載の電子メールシステム。

【請求項５】　前記中継サーバは、前記外部ドメインで表された宛先を示す宛先情報に対応付けて、前記配布リスト及び前記ファイル証明書の有無により電子メールの送信を許可するための条件を表す送信条件と前記配布リスト及び前記ファイル証明書を前記外部ドメインに送信すべきか削除すべきを表す送信処理削除との各情報を格納した送信制御テーブルと、

前記端末から送られてくる前記電子メールに付加された情報と前記送信制御テーブルに格納された各情報とに基づいて前記外部ドメインへの前記電子メールの送信可否を決定する送信制御部と、を備えることを特徴とする請求項３記載の電子メールシステム。

2

【請求項６】　外部ドメインとの間で電子メールを送受信する電子メール送信制御方法において、

端末が、電子メールを送受信し、

中継サーバが、前記端末からネットワークを介して電子メールを受信し、基本設定として前記外部ドメインへの前記電子メールの送信を禁止し、特定の条件が成立した場合に前記外部ドメインへの前記電子メールの送信を許可することを特徴とする電子メール送信制御方法。

【請求項７】　前記端末において、添付ファイルを作成する際に、この添付ファイルの内容を証明するファイル証明書を作成し、このファイル証明書に署名することにより添付ファイルとファイル証明書との関係及び内容を保証し、

前記中継サーバは、前記端末から送られてくる前記添付ファイルに付加された前記ファイル証明書及び署名の内容に基づいて前記外部ドメインへの前記電子メールの送信可否を決定し、許可された内容の電子メールのみを前記外部ドメインに送信することを特徴とする請求項６記載の電子メール送信制御方法。

【請求項８】　前記端末において、電子メールを送信する際に、電子メールの配布先及び配布内容を記載した配布リストを作成し、この配布リストに署名することにより電子メール本体と配布リストとの関係及び内容を保証し、

前記中継サーバは、前記端末から送られてくる前記電子メールに付加された前記配布リスト及び署名の内容に基づいて前記外部ドメインへの前記電子メールの送信可否を決定し、許可された内容の電子メールのみを前記外部ドメインに送信することを特徴とする請求項６又は請求項７記載の電子メール送信制御方法。

【請求項９】　前記端末において、前記配布リストにより配布リストと電子メール本体と前記添付ファイルとの関係を保証し、前記ファイル証明書により前記添付ファイルと前記ファイル証明書との関係を保証し、前記配布リストと前記ファイル証明書との関係を前記添付ファイルを介して間接的に保証することにより、必要に応じて前記添付ファイル証明書又は前記配布リストを削除しても個々の保証関係に問題を生じないことを特徴とする請求項８記載の電子メール送信制御方法。

【請求項１０】　前記中継サーバは、前記外部ドメインで表された宛先を示す宛先情報に対応付けて、前記配布リスト及び前記ファイル証明書の有無により電子メールの送信を許可するための条件を表す送信条件と前記配布リスト及び前記ファイル証明書を前記外部ドメインに送信すべきか削除すべきを表す送信処理削除との各情報を送信制御テーブルに格納し、

前記端末から送られてくる前記電子メールに付加された

情報と前記送信制御テーブルに格納された各情報とに基づいて前記外部ドメインへの前記電子メールの送信可否を決定することを特徴とする請求項８記載の電子メール送信制御方法。

【請求項１１】　電子メールを送受信する端末と外部ドメインとの間に設けられ、前記端末と前記外部ドメインとの間で電子メールを送信制御する中継装置であって、前記端末からネットワークを介して電子メールを受信し、基本設定として前記外部ドメインへの前記電子メールの送信を禁止し、特定の条件が成立した場合に前記外部ドメインへの前記電子メールの送信を許可する送信制御部を備えることを特徴とする中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、外部ドメインとの間で電子メールを送受信する電子メールシステム及び電子メール送信制御方法並びに中継装置に関し、特に電子メールに添付する証明書と中継サーバにおける電子メールの送信制御に関する。

【０００２】

【従来の技術】従来の電子メールシステムにおいて、特にローカルエリアネットワーク（以下、ＬＡＮと称する。）に接続され、インターネット等を介して外部ドメインとの間で、電子メールの送受信を行う電子メールシステムでは、基本設定として外部ドメインに対する電子メールの送信を許可しておくのが一般的であった。この理由は、外部ドメインに対する送信制御を電子メール個々について制御する手軽な手段がないからである。

【０００３】この場合、本来は外部ドメインに送信されてはならない電子メールや添付ファイルが、電子メールシステムの利用者の操作ミスなどにより、誤って送信されてしまう欠点があった。

【０００４】近年、電子メールシステムが重要なビジネスツールに位置付けられた結果、このような欠点を補う方法として、いわゆる「コンテンツセキュリテイ」が考案されている。これは、電子メールの内容や添付ファイルの内容を電子メールの中継装置が確認し、電子メール中に特定の単語や文章表現が含まれている場合に、電子メールの社外への送信を禁止するものである。

【０００５】

【発明が解決しようとする課題】しかしながら、このような方式は、「特定の条件が成立すれば、電子メールの送信を禁止する」ものであり、特定の条件が成立しなければ、電子メールが送信されてしまう。このため、利用者が、特定の単語や文章表現を電子メールや添付ファイルに設定するのを忘れてしまうと、結果として、情報が社外に流出してしまう欠点があった。

【０００６】また、この「コンテンツセキュリテイ」において、デホルトの設定を社外送信禁止として、「社外送信可」等の特定の文言がある場合に社外送信を許可する方式もある。しかし、特定の文言の記入が電子メール作成者に依存しているため、勘違いや故意の操作に対して電子メールが保護されない欠点があった。

【０００７】本発明は、基本的に外部への電子メールの送信を禁止とし、特定の条件が成立した場合のみ外部への電子メールの送信を許可し、電子メールに添付する証明書や配布リストと電子署名により電子メールの送信の厳密性を保証するとともに、添付する証明書の判定の厳密性を変えることにより、ポリシーに応じて使いやすさと安全性程度を選択できる電子メールシステム及び電子メール送信制御方法並び中継装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、外部ドメインとの間で電子メールを送受信する電子メールシステムにおいて、電子メールを送受信する端末と、この端末からネットワークを介して電子メールを受信し、基本設定として外部ドメインへの電子メールの送信を禁止し、特定の条件が成立した場合に外部ドメインへの電子メールの送信を許可する中継サーバとを備えることを特徴とする。

【０００９】また、本発明は、電子メール本体や添付ファイルにより情報交換が行われる場合に、電子メールの作成から送信に至る過程で、情報作成者、情報管理責任者、情報配布者の３つの役割を想定し、配布リストやファイル証明書をディジタル署名により保証し、中継サーバがこの情報を用いて外部ドメインへの送信を許可するものである。

【００１０】すなわち、端末において、添付ファイルを作成する際に、この添付ファイルの内容を証明するファイル証明書を作成し、このファイル証明書に署名することにより添付ファイルとファイル証明書との関係及び内容を保証し、中継サーバは、端末から送られてくる添付ファイルに付加されたファイル証明書及び署名の内容に基づいて外部ドメインへの電子メールの送信可否を決定し、許可された内容の電子メールのみを外部ドメインに送信することを特徴とする。この際、添付ファイルとファイル証明書の添付ファイル属性部分の二つのハッシュ値を連結して用いて、添付ファイルと証明書の関係を保証する。

【００１１】また、端末において、電子メールを送信する際に、電子メールの配布先及び配布内容を記載した配布リストを作成し、この配布リストに署名することにより電子メール本体と配布リストとの関係及び内容を保証し、中継サーバは、端末から送られてくる電子メールに付加された配布リスト及び署名の内容に基づいて外部ドメインへの電子メールの送信可否を決定し、許可された内容の電子メールのみを外部ドメインに送信することを特徴とする。

【００１２】また、中継サーバは、署名と配布リスト及

5

びファイル証明書の内容に基づいて外部ドメインへの送信可否を決定し、許可された内容の電子メールのみを外部ドメインに送信しても良い。この際、電子メール本体と添付ファイルと配布リストの三つのハッシュ値を連結して用いて、電子メール本体と配布リストと添付ファイルの関係を保証し、ファイル証明書との関係はファイル証明書の署名により添付ファイルを介して間接的に保証する。

【００１３】以上のように、本発明は、「特定の条件が成立すれば外部への送信を許可する」ことを基本設定とし、電子メールに添付するファイル証明書や配布リストと電子署名により、これらの厳密性を保証するとともに、添付するファイル証明書の判定の厳密性を変えることにより、運用方針（ポリシー）に応じて使いやすさと安全性の程度を選択できる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態の電子メールシステム及び電子メール送信制御方法並びに中継装置を図面を参照しながら詳細に説明する。実施の形態の電子メールシステムは、電子メール本体や添付ファイルにより外部ドメインとの間で情報交換が行われる場合に、電子メールの作成から送信に至る過程で、情報作成者、情報配布者、情報管理責任者の３つの役割を想定し、ファイル証明書や配布リストをディジタル署名により保証し、中継サーバがこれらの情報を用いて外部ドメインへの電子メールの送信を許可することを特徴とする。

【００１５】図１は本発明の実施の形態に係る電子メールシステムを示す構成図である。図１に示す電子メールシステムは、内部ドメインにＬＡＮ１を有し、このＬＡＮ１には、情報作成者が所有する情報作成者端末２と、情報配布者が所有する情報配布者端末３と、情報取り扱い責任者が所有する情報取り扱い責任者端末４と、電子メールサーバ５と、中継サーバ６（本発明の中継装置に対応）とが接続されて構成される。なお、情報作成者、情報配布者、情報取り扱い責任者は、電子メールクライアントである。

【００１６】各端末２，３，４は、図２に示すように、電子メールのための情報を入力するキーボードやマウス等の入力部２０２、前記情報を記憶する記憶部２０３、前記情報を表示する表示部２０４、電子メールの送受信を行う通信装置２０５、処理プログラム２０７を格納するリードオンリーメモリ（ＲＯＭ）２０６、これらの各部を制御する中央処理装置（ＣＰＵ）２０８を有して構成される。

【００１７】情報作成者端末１は、情報作成者が添付ファイルを作成したり、添付ファイルの内容を証明するファイル証明書を作成するもので、ファイル証明書の作成の詳細については、後述する。情報配布者端末２は、情報配布者が配布リストを作成するもので、この配布リストの作成の詳細については、後述する。情報取り扱い責任者端末４は、情報取り扱い責任者が情報作成者や情報配布者が作成した配布リストやファイル証明書の検証を行う。

6

【００１８】電子メールサーバ５は、内部ドメインの電子メールサーバで、クライアントの電子メールを宛先用のメールボックスに保管するもので、クライアントのメーラーから社外向けの電子メールを受信し、電子メールの宛先を確認し、ドメイン外への電子メールの場合には中継サーバ５へ送信する。

【００１９】中継サーバ６は、例えば、ゲートウェイ等からなり、外部ドメインへの電子メールを送信するサーバであり、基本設定として外部ドメインへの電子メールの送信を禁止し、特定の条件が成立した場合に外部ドメインへの電子メールの送信を許可するもので、詳細は後述する。中継サーバ６は、図３に示すように、情報を入力するキーボードやマウス等の入力部６０２、外部ドメインへ電子メールを送信すべきか否かを表すための送信制御情報を格納した送信制御テーブル６１を有するデータベース６０３、情報を表示する表示部６０４、電子メールの送受信を行う通信装置６０５、送信制御テーブル６１の送信制御情報に基づき電子メールの外部ドメインへの送信を制御する送信制御部６２、これらの各部を制御するＣＰＵ６０８を有して構成される。

【００２０】以上の説明では、電子メールシステムの概略構成を述べたが、以下の説明では、各端末の処理、中継サーバの処理をより詳細に述べるものとする。

【００２１】（ファイル証明書）まず、情報作成者端末２における処理、すなわち、情報作成者によるファイル証明書の作成について説明する。図４は電子メールでの送信を前提とした電子ファイルとファイル証明書の関係を示す図である。情報作成者端末２において、電子ファイル１１の情報作成者が電子ファイル１１の内容を証明するファイル証明書１２を作成し、ファイル証明書１２に、ファイル名やファイルサイズ、作成日、作成者、有効期限、外部提出の可否などをファイル属性１３として記入する。また、ファイル証明書１２に、ファイル属性部分のハッシュ値と電子ファイル１１が有するハッシュ値とを結合（ハッシュ値の結合１４）して、情報作成者の秘密鍵によりディジタル署名１５を付加する。ハッシュ値の結合は、二つの値を単に並べるだけでも、数学的な演算処理を施しても良いが、それぞれの値が個々に検証可能な方式が望ましい。

【００２２】情報作成者は、ディジタル署名１５をファイル証明書１２に付加した後、情報作成者端末２から情報取り扱い責任者端末４への電子メールの送信あるいは、フロッピー（登録商標）ディスクなどの手段によって情報取り扱い責任者に申請する。

【００２３】電子ファイル１１とファイル証明書１２を受領した情報取り扱い責任者は、ファイル証明書１２と

電子ファイル１１の内容を確認し、情報作成者の公開鍵により復号したハッシュ値と、電子ファイル１１とファイル証明書１２から新たに求めたハッシュ値とが一致していることにより、ファイル証明書１２の内容と電子ファイル１１との関係を検証する。

【００２４】情報取り扱い責任者は、上記の検証によりこれらの関係を検証した後、情報取り扱い責任者の秘密鍵によりディジタル署名１７をファイル証明書１２に付加する。この時、ファイル属性部分のハッシュ値と情報作成者の署名のハッシュ値を結合（ハッシュ値の結合１６）してディジタル署名を行う。

【００２５】なお、電子ファイル本体のハッシュ値を新たに求めても良いが、情報作成者の署名のハッシュ値により間接的に保証できる。また、ファイル属性部分と情報作成者の署名の部分を一体として新たにハッシュ値を求めてこれをディジタル署名に使用しても良い。

【００２６】ファイル証明書１２は、電子メールに添付することを前提としたものであるが、電子メールに限定する必要はなく、純粋に電子ファイル１１に対する証明書と考えても良い。

【００２７】（配布リスト）次に、情報配布者端末３における処理、すなわち、情報配布者による配布リストの作成について説明する。図５は電子メールと配布リストの関係を示す図である。情報作成者と情報配布者とが同一人の場合を想定し、配布リスト２２によって電子メール２１の内容を保証し、情報取り扱い責任者が電子メール２１の内容を確認し、配布リスト２２に署名することにより電子メール２１の内容が外部に配布して問題ないことを保証する。

【００２８】まず、情報作成者が配布リスト２２を作成し、この配布リスト２２に電子メールの配付先や配布内容２３を記入する。この配布リスト２２に、配付先・配布内容部分のハッシュ値と電子メール自体のハッシュ値を結合（ハッシュ値の結合２４）して、情報作成者の秘密鍵によりディジタル署名２５を付加する。電子メール２１のハッシュ値はメール本文２１ａだけでも良いが、題名２１ｂのハッシュ値も結合すれば、電子メール２１の全ての記入可能な領域の完全性を保証できるため、より厳密な保証を行うことができる。

【００２９】電子メール２１と配布リスト２２を受領した情報取り扱い責任者は、配布リスト２２と電子メール２１の内容を確認し、検証によりこれらの関係を確認した後、情報取り扱い責任者の秘密鍵によりディジタル署名２７を配布リスト２２に付加する。この時、配布リスト２２の配付先・配布内容のハッシュ値と情報作成者の署名のハッシュ値を結合（ハッシュ値の結合２６）してディジタル署名を行う。電子メールのハッシュ値を新たに求めても良いが、情報作成者の署名のハッシュ値により間接的に保証できる。

【００３０】（配布リストと添付ファイル）次に、添付

ファイル及び配布リストの作成について説明する。図６は電子メールと添付ファイルと配布リストの関係を示す図である。図５と同様に情報作成者と情報配布者とが同一人である場合で、一時的に添付ファイル１１ａを作成する場合を想定している。

【００３１】まず、情報作成者がファイルの配布リスト２２を作成し、この配布リスト２２に配付先や配布内容を記入する。この配布リスト２２に、配付先・配布内容部分のハッシュ値と電子ファイル自体のハッシュ値と添付ファイル１１ａのハッシュ値を結合（ハッシュ値の結合２４ａ）して、情報作成者の秘密鍵によりディジタル署名２５を付加する。

【００３２】電子メール２１と配布リスト２２と添付ファイル１１ａを受領した情報取り扱い責任者は、配布リスト２２と電子メール２１と添付ファイル１１ａの内容を確認し、検証によりこれらの関係を確認した後、情報取り扱い責任者の秘密鍵によりディジタル署名２７を配布リスト２２に付加する。

【００３３】（配布リストとファイル証明書）次に、図７を参照して添付ファイルにファイル証明書が付く場合について説明する。配布リスト２２の署名の情報に、ファイル証明書１２の有無に関する情報（ファイル証明書１２のハッシュ値）を明記しなければ、ファイル証明書１２を削除しても保証関係は崩れない。ファイル証明書１２を削除しないことを保証する場合は、配布リスト２２にファイル証明書１２があることを、ファイル証明書１２のハッシュ値により明記すればよい。

【００３４】ファイル証明書１２や配布リスト２２の確認と保証のために行われる情報取り扱い責任者とのやり取りは、フロッピーディスクであっても電子メールを利用しても良い。情報取り扱い責任者が署名した内容と同じであれば、保証関係は維持される。この検証は、情報取り扱い責任者の公開鍵を用いて行うことができるので、情報作成者や情報配布者が確認することもできる。

【００３５】最終的には、電子メール２１、配布リスト２２、添付ファイル１１ａ、ファイル証明書１２の４つがそろった状態で、電子メールとして発行される。この電子メールを中継サーバ６が検証して、外部送信可能と判定されたものだけを外部に送信する。その際に、必要に応じて、配布リスト２２やファイル証明書１２を削除することができる。

【００３６】（証明書や配布リストの削除に対する考慮）また、図７に示す例では、配布リスト２２に設けられた署名２７により、配布リスト２２と電子メール２１（本発明の電子メール本体に対応）と添付ファイル１１ａとの関係を保証している。ファイル証明書１２に設けられた署名１７により、添付ファイル１１ａとファイル証明書１２との関係を保証している。

【００３７】さらに、配布リスト２２の署名２７に、ファイル証明書１２のハッシュ値を用いず、配布リスト２

２とファイル証明書１２との関係を添付ファイル１１ａを介して間接的に保証するように構成することで、必要に応じて、ファイル証明書１２を削除することができる。これにより、必要に応じて、添付ファイル証明書１２を削除しても、配布リスト２２と電子メール２１と添付ファイル１１ａとの保証関係に問題を生じない。

【００３８】また、必要に応じて、電子メール作成者のディジタル署名だけを用いて電子メール２１に署名することもできるため、配布リスト２２を削除しても作成者のディジタル署名（電子メール２１中の作成者署名）を残すこともできる。また、必要に応じて、配布リスト２２を削除しても、添付ファイル１１ａとファイル証明書１２との保証関係に問題を生じない。このため、このようなファイル証明書１２や配布リスト２２を用いた管理が行われていることを社外に対して秘密にすることもできる。さらに、電子メール２１や添付ファイル１１ａとは独立したファイル証明書１２や配布リスト２２を用いるため、管理方針に基づき、情報管理責任者の機能を情報作成者や情報配布者に統合し、セキュリテイを緩和する代わりに利便性を高めるなど、使いやすさと安全性の程度を選択可能とすることができる。

【００３９】（中継サーバ）次に、中継サーバの処理について説明する。中継サーバー６は、基本的に外部ドメインへの電子メールの送信を禁止し、予め設定されたドメインには無条件で電子メールの送信を許可する。中継サーバ６は、外部ドメインに対して電子メールの送信要求がある場合には、ドメイン毎に設定された電子メール送信制御ポリシー（以下、ポリシーと称する。）に応じて、電子メール本体、配布リスト２２、ファイル証明書１２、添付ファイル１１ａの整合性と内容を確認し、宛先ドメインに対して送付可能なものを送信し、それ以外はコメントを付加して送信元に返送する等の処置を行う。

【００４０】前記ポリシーは、前述した送信制御テーブル６１により設定される。図８は中継サーバに設けられた送信制御テーブル（以下、ＴＣＬと称する。）６１を示す図である。このＴＣＬ６１は、宛先情報に応じて送信条件の設定や送信時のファイル証明書の扱い等を一覧表に設定したもので、より具体的には、外部ドメインで表された宛先を示す宛先情報に対応付けて、配布リストやファイル証明書の有無により電子メールの送信を許可するための条件を表す送信条件と、資料の取り扱い区分を表す資料区分と、送信処理削除と、送信不可通知の各情報を格納したものである。

【００４１】（宛先情報及び送信条件の設定）宛先情報は、図８に示すように、例えば、「*@aaa.co.jp」、「*@bbb.co.jp」、「*@ccc.co.jp」、「*@ddd.co.jp」の４つのドメインと、「Etc」である。宛先情報が「*@aaa.co.jp」である場合には、送信条件の配布リストのフラグを‘０’（‘０’は配布リストを必須とせず、‘１’は配布リストを必須とする。）、ファイル証明書のフラグを０（‘０’はファイル証明書を必須とせず、‘１’はファイル証明書を必須とする。）に設定している。端末から受信した電子メールがこの送信条件を満足する場合には、社内と同様に無条件に電子メールの外部ドメインへの送信を許可する。

【００４２】宛先情報が「*@bbb.co.jp」である場合には、配布リストを必須とし、宛先情報が「*@ccc.co.jp」である場合には、配布リスト２２とファイル証明書１２を必須とし、宛先情報が「*@ddd.co.jp」である場合には、ファイル証明書１２だけを必須とし、「Etc」すなわち、その他の外部ドメインには、配布リスト２２とファイル証明書１２を必須とするように送信条件の各フラグが設定されている。

【００４３】このように、中継サーバ６は、内部／外部という判定でなく、ドメインで設定が可能で、外部であっても、ある特定ドメインに対しては、内部と同様に自由な電子メール送信を許可することもできる。また、ドメイン別に送信条件を変えることで、電子メール送信を許可することもできる。

【００４４】（資料区分の設定）前記資料区分は、配布リスト２２及びファイル証明書１２に記述する資料の取り扱い区分であり、ＴＣＬ６１の資料区分には、「一般」、「社外秘」、「部外秘」がある。資料区分のフラグが‘０’である場合には、電子メールの外部ドメインへの送信を許可し、資料区分のフラグが‘１’である場合には、電子メールの外部ドメインへの送信を不可とする。

【００４５】資料区分としては、企業組織のポリシーに応じて各種の区分が可能である。一般的に、企業内では、「部外秘」、「社外秘」、「取り扱い注意」、「一般資料」などの資料区分がある。配布リスト２２とファイル証明書１２にはこれらの資料区分が記載され、ディジタル署名により保護される。

【００４６】例えば、次のような資料区分の設定が一般的である。配布リストやファイル証明書がない電子メールの社外ドメインへの送信は一切拒否する。「部外秘」、「社外秘」、「取り扱い注意」等の区分がある場合も同様に、社外ドメインへの送信を拒否する。送信が許可されるのは「一般資料」だけである。これらの区分のどれに該当するかは、情報作成者あるいは情報配布者が選択し情報取り扱い責任者が確認する。

【００４７】本来、「部外秘」の資料を扱う部門では、配布リストもファイル証明書もなしで、自由に電子メールを交換できる範囲は部内だけであり、社内であっても、他の部と電子メールの交換を行う場合は配布リストとファイル証明書が必要になる。但し、運用効率に着目して中継サーバ６の管理を緩め、社内であれば情報取り扱い責任者のディジタル署名は不要とし、情報作成者あるいは情報配布者の署名だけで送信を許可するなど、部

門のポリシーに応じた設定とすることができる。また、特に運用効率を重視すれば、社内は部内と同様に自由に電子メールを交換できるものとし、個人の注意に任せることもできる。

【００４８】（送信処理削除及び送信不可通知の情報の設定）図８に示す送信処理削除の情報は、中継サーバ６が受信した電子メールを外部へ送信する際に、電子メールに付加された配布リストやファイル証明書を削除するかどうかを表す情報である。送信処理削除のフラグが‘０’である場合には、配布リストやファイル証明書を削除せず、送信処理削除のフラグが‘１’である場合には、配布リストやファイル証明書を削除するものとする。この送信処理削除のフラグにより、電子メールの外部への送信時に、配布リスト２２及びファイル証明書１２を削除する等の設定ができる。

【００４９】図８に示す送信不可通知の情報は、電子メールを外部へ送信しない場合に、送信元や情報取り扱い責任者に対して、電子メールの送信不可を通知するかどうかを表す情報である。送信不可通知のフラグが‘０’である場合には、通知せず、送信不可通知のフラグが‘１’である場合には、通知するものとする。

【００５０】（配布リストの管理）情報の管理を行うためには、最低限、情報配布者のディジタル署名が付加される必要がある。Ｓ／ＭＩＭＥ（Secure Multipurpose Internet Mail Extensions）やＰＧＰ（Pretty Good Privacy）などは、電子メール本体に個人のディジタル署名を付加する機能があるが、題名や配布先まで署名の対象にならない場合が多く、電子メールの情報管理としては不完全である。配布先や題名を署名による保護の対象としながら、必要に応じて証明書や配布リストを削除できるようにするためには、「配布リスト」を電子メール本体とは別の資料として扱う必要がある。

【００５１】中継サーバ６は、配布リストやファイル証明書を含み送信時の削除の有無等も含む形式でログとして記録保管することにより完全な情報管理が可能になる。

【００５２】次に、中継サーバの外部ドメインへの電子メールの送信制御を図９に示すフローチャートを参照しながら説明する。

【００５３】まず、情報配布者から内部ドメインの電子メールサーバ５に送信された電子メールは、送信先が外部ドメインの場合は、中継サーバ６に送信される。中継サーバ６が電子メールサーバ５から外部送信メールを受信すると（ステップＳ１１）、このメールの中から宛先情報を読み出す（ステップＳ１３）。そして、送信制御部６２は、ＴＣＬ６１を参照して、メールから読み出した宛先情報とＴＣＬの宛先情報とを照合する。すなわち、図８に示す例では、上の行から順番に宛先情報の照合を行う。テーブルの最後に「Etc」と書かれているのは、それより上の行に該当しなかった場合に「Etc」

（その他のすべての宛先）に対して行う処理が書かれている。「Etc」を設定する代わりにテーブルのデホルト処理を別に決めておいても良い。「Etc」の記述がある場合はそちらを優先する。「*@aaa.co.jp」等の先頭の「*」は「何でも良い」を意味するワイルドカードである。「*」の代わりに特定のアドレスを書けば、ドメインでなく個別のアドレスに対してコントロールすることもできる。

【００５４】次に、送信制御部６２は、メール中の宛先情報をＴＣＬ６１から検索した場合には、検索された宛先情報に対応する送信条件、資料区分、送信処理削除、送信不可通知の各情報を読み出す（ステップＳ１５）。

【００５５】次に、送信制御部６２は、メールに付加された情報（以下、メール情報と称する。）が送信条件情報を満足するかどうかを判定する（ステップＳ１７）。メール情報が送信条件情報を満足する場合とは、例えば宛先情報が「*@bbb.co.jp」である場合に、メール中に配布リストが付加されており、送信条件の配布リストのフラグが‘１’の場合である。

【００５６】次に、メール情報が送信条件情報を満足する場合には、送信制御部６２は、メール情報が資料区分情報を満足するかどうかを判定する（ステップＳ１９）。メール情報が資料区分情報を満足する場合とは、例えば宛先情報が「*@bbb.co.jp」である場合に、メール中に「部外秘」の資料が付加されており、資料区分の「部外秘」のフラグが‘１’の場合である。

【００５７】さらに、送信制御部６２は、送信処理削除の情報、すなわち、フラグに基づき配布リスト、ファイル証明書を削除するかどうかを判定し（ステップＳ２１）、フラグが‘１’である場合には、配布リスト、ファイル証明書を削除して（ステップＳ２３）、メールを外部ドメインに送信する（ステップＳ２５）。また、フラグが‘０’である場合には、配布リスト、ファイル証明書を削除しないでメールを外部ドメインに送信する（ステップＳ２５）。

【００５８】一方、ステップＳ１７でメール情報が送信条件情報を満足しない場合、あるいはステップＳ１９でメール情報が資料区分情報を満足しない場合には、送信元や情報取り扱い責任者に送信不可通知を行う（ステップＳ２７）。

【００５９】以上の説明では、中継サーバの基本的な送信制御を述べたが、次に、図８に示すＴＣＬ６１の具体的な設定例での中継サーバの送信制御を説明する。

【００６０】まず、先頭の「*@aaa.co.jp」では、社内（あるいは内部ドメイン）と全く同じく、送信条件として、配布リスト、ファイル証明書ともに必須ではない。このため、「*@aaa.co.jp」の宛先に対しては、ファイル証明書を一切付けずに電子メールを送信することができる。この場合、配布リスト、ファイル証明書のいずれも削除されない。仮に、証明書が付いていても削除され

ない。また、ここでは発生しないはずだが、送信不可と判定された場合の「送信不可通知」は、送信元のみに返され、情報取り扱い責任者には返されない。このドメインは、社内（あるいは内部ドメイン）と同等の扱いであり、「資料区分」の「一般」「社外秘」「部外秘」の全てを送信可とする。「資料区分」の確認は一切行われない。

【００６１】２行目の「*@bbb.co.jp」では、「配布リスト」が必須で、「ファイル証明書」は必須ではない。従って、「配布リスト」の署名検証のみ行われる。送信処理では検証済みの「配布リスト」を削除するとともに、仮に「ファイル証明書」が添付されていた場合は、これも削除する。このドメインは、ほぼ社内と同等の扱いであるが全面的には信頼できないドメインであり、「資料区分」の「一般」のみが送信許可される。「配布リスト」により情報取り扱い責任者によるメール内容の確認が行われており、社外秘程度までの送信を許可する。「社外秘」と「一般」の資料区分は「配布リスト」内の記述により確認する。

【００６２】３行目の「*@ccc.co.jp」では、「配布リスト」と添付ファイルがある場合は「ファイル証明書」との両方が必須で、「配布リスト」と添付ファイルがある場合は「ファイル証明書」の両方の署名の検証が行われる。送信処理では検証済みの「配布リスト」と「ファイル証明書」の両方を削除する。この宛先の場合は、送信不可通知を送信元だけでなく、情報取り扱い責任者に対しても行う。特殊な注意を要する宛先の一例である。このドメインは社外の特殊顧客等であり、「資料区分」の「一般」のみが送信可能である。

【００６３】４行目の「*@ddd.co.jp」では、添付ファイルがある場合に「ファイル証明書」が必須で、「配布リスト」は必須ではない。電子メールの本文と添付ファイルの関係は、特にチェックしなくても良いが、添付ファイルだけは確認しておきたい場合の一例である。もし、配布リストが付いていれば削除し、ファイル証明書はそのまま添付する。配布する添付ファイルの信憑性を保証する必要がある宛先である。

【００６４】このドメインは、ほぼ社内と同等の扱いで、かなり信頼できる。打合せのためメールの交換能率をある程度高める必要があるドメインで、「資料区分」の「社外秘」程度まで送信許可される。通常は添付ファイルを用いないことで「部外秘」の漏洩を防ぐ。仮に「部外秘」が漏洩しても致命的な問題にはならない。むしろ、配布先に対してファイルの信憑性を保証する必要がある。「配布リスト」は必要としないので比較的自由なメール送信が可能であるが、添付ファイルがある場合はファイル証明書が必要になる。電子メール本文は暫定的な意見交換で、添付ファイルが正式文書となる。

【００６５】以上は、ＴＣＬ６１の一例であるが、さらに、各証明書の内部情報に踏み込んで、署名の組合せや

ファイルの作成日ファイル名などをチェックすることもできる。このようなメールポリシーを設定することにより、必要に応じて安全なメール送信を保証することができる。

【００６６】以上説明したように、中継サーバ６は、電子メールの内容と配付先が予め設定されたドメインの電子メールポリシーに適合しているかどうかを確認し、適合している場合は予め設定された処理を行った後に外部ドメインの電子メールサーバに送信する。適合していなかった場合は、適合しなかった内容を指摘するコメントを電子メールに付加して送信元に返送する等、予め決められた処理を行う。

【００６７】以上の一連のシステム処理によって、ドメインの電子メールポリシーに適合しない電子メールが誤って外部ドメインに送信される危険を防止できる。

【００６８】また、中継サーバ６によって、日常的に電子メールの交換が必要な社内あるいは社外の関係者とは、無条件あるいは簡易的な条件で電子メールの交換を行いながら、電子メールの扱いに注意が必要な外部ドメインに対しては、仮にクライアントで処理を間違えても電子メールの送信を拒否でき、安心して利用できる電子メールシステムを構築できる。

【００６９】また、中継サーバ６の検証条件は、システムの方針に応じて、簡略化することができる。例えば、ファイル証明書１２をなくし、配布リスト２２だけで管理することもでき、配布リスト２２を配布者自信の署名だけで送信することもできる。配布リスト２２の作成と管理を電子メールの作成者に任せても、配布リスト２２を作成する行為の過程で、作成者に注意を促すことにより、誤って重要情報を外部に送信する危険性を低減することができる。

【００７０】また、このような配布リスト２２やファイル証明書１２は、内部では必ずしも必要とせず、外部に送信する場合にだけ必要となるため、通常の業務に与える能率低下などの影響を低減させることができる。

【００７１】（署名／検証ツール）次に、署名及び検証ツールについて説明する。ファイル証明書１２や配布リスト２２を作成しディジタル署名するためには、専用の検証ツールを用いる方が取り扱いが容易である。この検証ツールは、各端末２，３，４に設けられた署名及び検証を実施するための処理プログラム２０７であり、この処理プログラム２０７を実行することで署名及び検証を行うことができる。

【００７２】図１０は署名／検証ツールのトップメニューを示す図である。この検証ツールには、画面上に表示された「ファイル証明書」ボタンＢ１と「配布リスト」ボタンＢ２と「電子メール検証」ボタンＢ３と「終了」ボタンＢ４との４つのボタンがある。電子メール検証の場合には、ツール起動時に選択されている電子メールあるいは、「電子メール検証」ボタンＢ３を選択した後に

15

「電子メール」を選択することにより、選択した電子メールの「電子メール」「添付ファイル」「配布リスト」「ファイル証明書」の全体について検証を行い、結果としてそれぞれの署名者とその整合性を表示する。また、「終了」ボタンB4を選択することで「署名/検証ツール」を終了する。細部の記入項目は、適用業務に応じたテンプレートを予め作成しツールに登録して用いる。

【0073】図11は署名/検証ツールのトップメニューから「ファイル証明書」ボタンB1を選択した後のメニューツリーを示す図である。一段目のメニューには「作成/修正」ボタン11、「署名」ボタン15、「検証」ボタンB18、「保存」ボタン21、「読み込み」ボタン22、「申請」ボタン24、「終了」ボタン25が表示されている。「作成/修正」ボタン11は、ファイル証明書12の作成を行うモードで、次に「ファイル選択」ボタン12の画面が表示される。予めファイルが選択されていればそのまま「記入」ボタン13の画面に移る。「記入」ボタン13の画面は、予め登録されたテンプレートにファイル個別の情報を記入する画面である。ファイル名、ファイルサイズ、ファイル作成日などの情報は、OSから取得し自動的に記入できるので、記入する情報は、ファイル作成者が判断しなければならない事項だけである。基本事項は、ファイルの取り扱い区分で、「部外秘」、「社外秘」、「取り扱い注意」、「一般資料」などの予め決められた区分を記入する。公開範囲として「部内限り」「社内限り」「一般公開可」等を用いる場合もある。具体的な区分は、組織のポリシーにより予め決めておく。全ての項目を記入し、「終了」ボタン14を選択することにより、元のメニューに戻る。

【0074】「署名」ボタン15は、ファイル作成者または情報取り扱い責任者のディジタル署名を付加する機能で、予め決められた権限で署名を付加する。署名は署名者の秘密鍵を用いて行うため、秘密鍵に登録されたパスフレーズを「パスフレーズ入力」ボタン16により入力しなければならない。パスフレーズの入力の代わりに、指紋入力などの個人識別手段を利用することもできる。ディジタル署名が付加されたファイル証明書は「保存/終了」ボタン17により、ファイルとして保存され、元のメニューに戻る。

【0075】「検証」ボタン18は、ファイル証明書12の署名を検証する機能で、ファイル証明書12の内容とディジタル署名の関係と内容を確認する。「ファイル作成者」と「情報取り扱い責任者」の二つの署名の有無とファイルのハッシュ値との関係を「ファイル作成者」と「情報取り扱い責任者」の公開鍵によって検証する。署名がなされていない場合は、署名がないことを表示する。「検証」は対象となるファイルを「ファイル選択」ボタン19により選択して行うが、予めファイルが選択されていればそのまま結果を表示して、「保存/終了」

16

ボタン20により、ファイルとして保存され、元のメニューに戻る。

【0076】「保存」ボタン21は、ファイル証明書12をファイルとして保存するボタンである。「読み込み」ボタン22は、作成途中のファイル証明書12を読み込むボタンである。ファイル証明書12またはファイルを選択して読み込む。ファイル証明書12が作成されていないファイルを「ファイル選択」ボタン23により選択すると、新規にファイル証明書12を作成する。

「申請」ボタン24は、予め指定された情報取り扱い責任者宛に、ファイルとファイル証明書12をメールで送信し証明を依頼・申請するボタンである。「終了」ボタン25により、署名/検証ツールのトップメニューに戻る。

【0077】図12は署名/検証ツールのトップメニューから「配布リスト」ボタンB2を選択した後のメニューツリーを示す図である。一段目のメニューには「作成/修正」ボタン31、「署名」ボタン35、「検証」ボタン38、「保存」ボタン41、「読み込み」ボタン42、「申請」ボタン44、「終了」ボタン46が表示されている。「作成/修正」ボタン31は、配布リストの作成を行うモードで、次に「電子メール選択」ボタン32の画面が表示される。予め電子メールが選択されていればそのまま「記入」ボタン33の画面に移る。「署名」ボタン35は、ファイル配布者または情報取り扱い責任者のディジタル署名を付加する機能で、予め決められた権限で署名を付加する。署名は署名者の秘密鍵を用いて行うため、秘密鍵に登録されたパスフレーズを「パスフレーズ入力」ボタン36により入力しなければならない。パスフレーズの入力の代わりに、指紋入力などの個人識別手段を利用することもできる。ディジタル署名が付加されたファイル証明書は「保存/終了」ボタン37により、ファイルとして保存され、元のメニューに戻る。

【0078】「検証」ボタン38は、配布リストの署名を検証する機能で、配布リストの内容とディジタル署名の関係と内容を確認する。「ファイル作成者」と「情報取り扱い責任者」の二つの署名の有無とファイルのハッシュ値との関係を「ファイル作成者」と「情報取り扱い責任者」の公開鍵によって検証する。署名がなされていない場合は、署名がないことを表示する。「検証」は対象となる電子メールを「電子メール選択」ボタン39により選択して行うが、あらかじめ電子メールが選択されていればそのまま結果を表示して、「保存/終了」ボタン40により、ファイルとして保存され、元のメニューに戻る。

【0079】「保存」ボタン41は、配布リストをファイルとして保存するボタンである。「読み込み」ボタン42は、作成途中の配布リストを読み込むボタンである。配布リストまたは電子メールを選択して読み込む。

ファイル証明書が作成されていない電子メールを選択すると、新規にファイル証明書を作成する。

【0080】「申請」ボタン44は、予め指定された情報取り扱い責任者宛に、電子メールと配布リストをメールで送信し証明を依頼・申請するボタンである。「メール送信」ボタン45は、情報取り扱い責任者から返送された配布リストと電子メール（添付ファイルがある場合は添付ファイルも）を、許可された配付先に電子メールで送信するボタンである。配付先を電子メールに新たに指定すると誤りの原因になるため、許可された配布リストから再生して使用する。この際、電子メールの内容と添付ファイルも、情報取り扱い責任者の返送メールから再生して作成することにより、許可された内容で確実に送信する。「終了」ボタン46により、署名／検証ツールのトップメニューに戻る。

【0081】以上説明したように、専用の検証ツールを用いることで、ファイル証明書12や配布リスト22を作成しディジタル署名することができ、取り扱いが容易となる。

【0082】（その他の実施例）図13は本発明の電子メールシステムをネットワークを介した電子メールサービスシステムに適用した場合の構成図である。このサービスシステムは、本発明をVPN（Virtual Private Network）などの安全なネットワークを介したサービスとして提供するものである。このサービスシステムは、作成者配布者端末2a、取り扱い責任者端末4a、電子メールサーバ5a、及びVPNゲートウェイ6aを有する電子メールシステムAと、作成者配布者端末2b、取り扱い責任者端末4b、電子メールサーバ5b、及びVPNゲートウェイ6bを有する電子メールシステムBと、VPNゲートウェイ7a，7b、中継サーバ8、及びFW（ファイア・ウォール）9を有する個別サービスエリアDと、この個別サービスエリアDとインターネットに接続される標準メール中継サーバ10とを有するインターネット接続サービスエリアCとを有して構成される。電子メールシステムAと電子メールシステムBとは、VPNゲートウェイ7a，7bを介して社内ネットワークを構築している。

【0083】以上の構成において、顧客（作成者、配布者、情報取り扱い責任者等）には、署名／検証ツールを提供し、顧客の電子メールを外部ドメインへ送信する場合には、インターネット経由でサービスドメインの中継サーバ8に送信させ、この中継サーバ8で外部ドメインに対する電子メールのポリシーによるファイルリングを行う。

【0084】大半のビジネス用途の場合、電子メールの社外送信を許可するかどうかを問題にすれば、重要情報の社外漏洩を防ぐことができるため、顧客の社内ネットワークでの電子メールはあまり規制する必要がない。この場合、社外に送信する電子メールだけを、本発明によるファイル証明書の構成により運用するようにすれば、社内の情報共有には運用効率の低下をもたらすことなく、安全な電子メールシステムを実現することができる。

【0085】なお、以上の実施例では、電子メールシステムを対象に説明したが、電子メール以外にもFTP（ファイル送信プロトコル）サービスなど、他のインターネット・サービスを用いる場合にも、本発明と同様のファイル証明書による技術が利用できる。この場合、対象となるサービスに適したツールを用いればよい。

【0086】

【発明の効果】以上説明したように、本発明によれば、基本的に外部への電子メールの送信を禁止とし、特定の条件が成立した場合のみ外部への電子メールの送信を許可し、電子メールに添付する証明書や配布リストと電子署名により電子メールの送信の厳密性を保証するとともに、添付する証明書の判定の厳密性を変えることにより、ポリシーに応じて使いやすさと安全性程度を選択することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る電子メールシステムを示す構成図である。

【図2】各端末の構成図である。

【図3】中継サーバの構成図である。

【図4】電子メールでの送信を前提とした電子ファイルとファイル証明書の関係を示す図である。

【図5】電子メールと配布リストの関係を示す図である。

【図6】電子メールと添付ファイルと配布リストの関係を示す図である。

【図7】添付ファイルにファイル証明書が付く場合の例を示す図である。

【図8】中継サーバに設けられた送信制御テーブルを示す図である。

【図9】中継サーバが外部送信メールを受信した場合における中継サーバの外部ドメインへの電子メールの送信制御を示すフローチャートである。

【図10】署名／検証ツールのトップメニューを示す図である。

【図11】署名／検証ツールのトップメニューからファイル証明書を選択した後のメニューツリーを示す図である。

【図12】署名／検証ツールのトップメニューから配布リストを選択したあとのメニューツリーを示す図である。

【図13】本発明の電子メールシステムをネットワークを介した電子メールサービスシステムに適用した場合の構成図である。

【符号の説明】

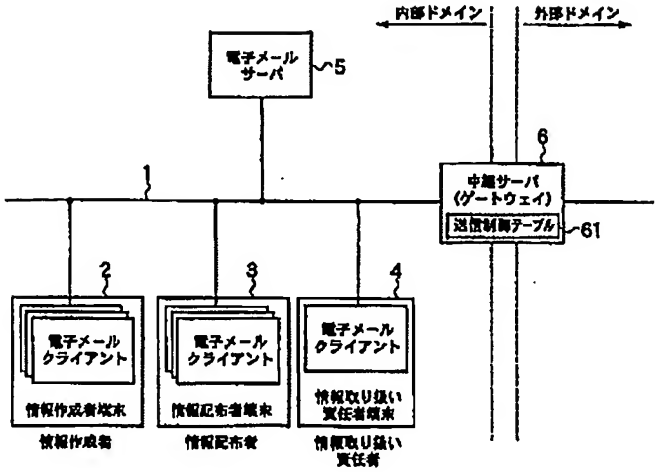
1…LAN、2…情報作成者端末、3…情報配布者端

19

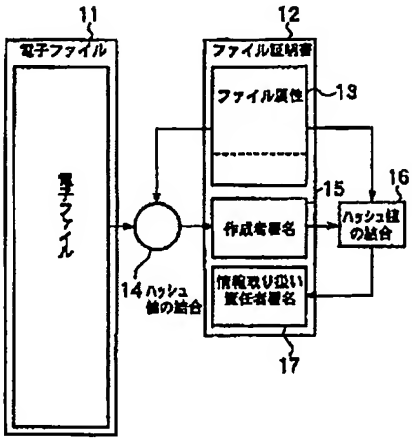
末、４…情報取り扱い者端末、５…電子メールサーバ、６…中継サーバ、１１…電子ファイル、１２…ファイル証明書、１３…ファイル属性、１５，２５…作成者署名、１７，２７…情報取り扱い責任者署名、２１…電子メール、２１ａ…メール本文、２１ｂ…題名、２２…配布先配布内容。

20

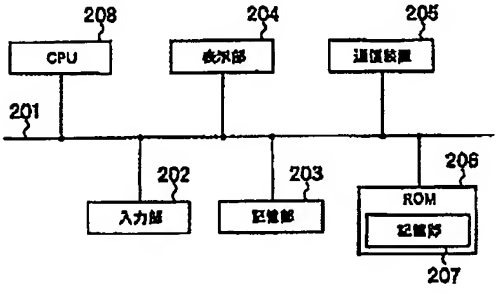
【図１】



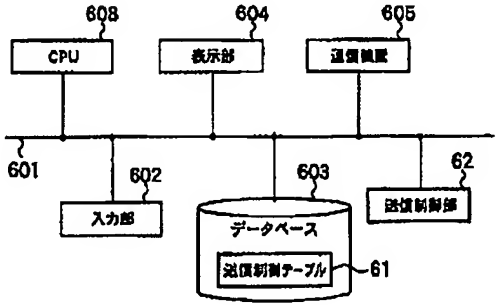
【図４】



【図２】



【図３】

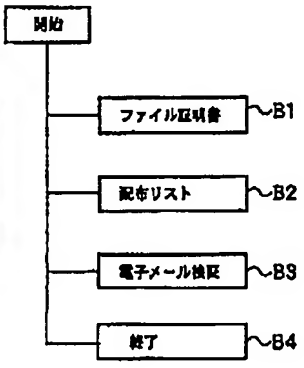


【図８】

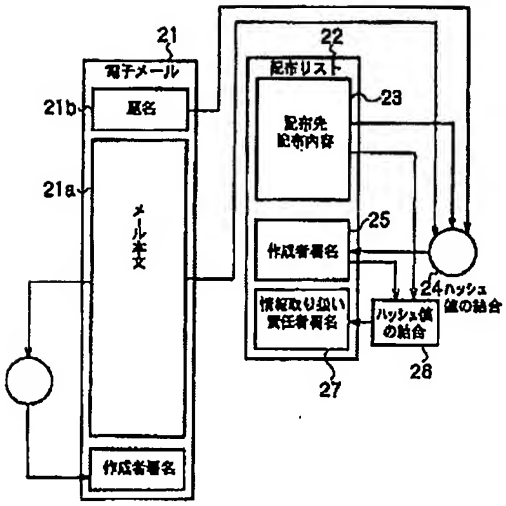
61 送信制御テーブル(TCL)

宛先情報	送信条件		資料区分			送信処理属性		送信不可通知	
	配布リスト	ファイル証明書	一般	社外秘	部外秘	配布リスト	ファイル証明書	送信元	責任者
*@aaa.co.jp	0	0	0	0	0	0	0	1	0
*@bbb.co.jp	1	0	0	0	1	1	1	1	0
*@ccc.co.jp	1	1	0	1	1	1	1	1	1
*@ddd.co.jp	0	1	0	0	1	1	0	1	0
Etc	1	1	0	1	1	1	1	1	0
	0：必須ではない 1：必須		0：送信可 1：送信不可			0：削除しない 1：削除する		0：通知しない 1：通知する	

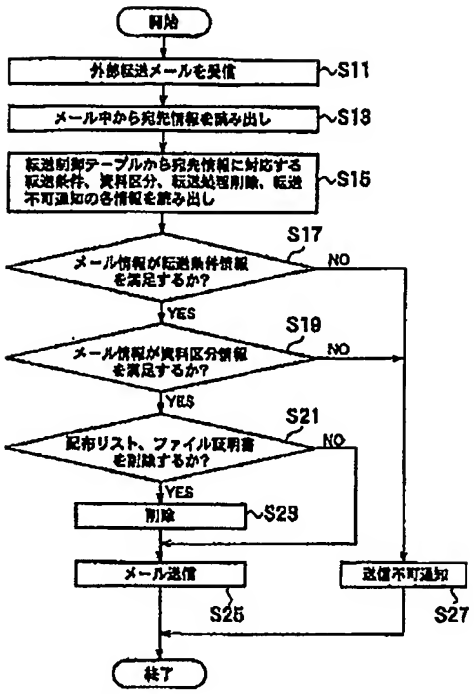
【図１０】



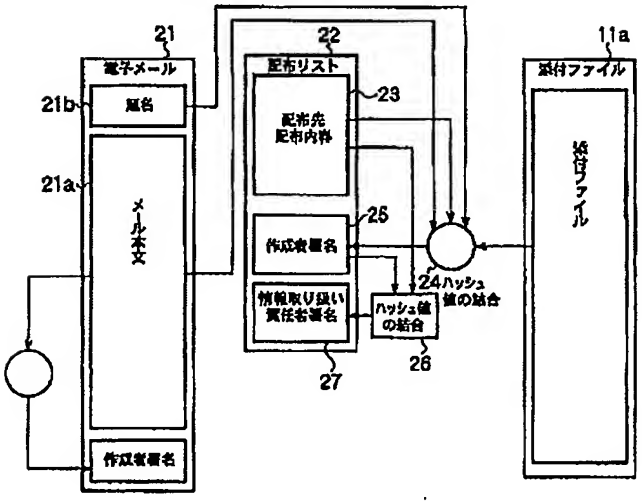
【図５】


21
電子メール
署名
21b
21a
メール本文
作成者署名
22
配布リスト
配布先
配布内容
23
作成者署名
25
情報取り扱い
責任者署名
ハッシュ値
の結合
24ハッシュ
値の結合
26
27

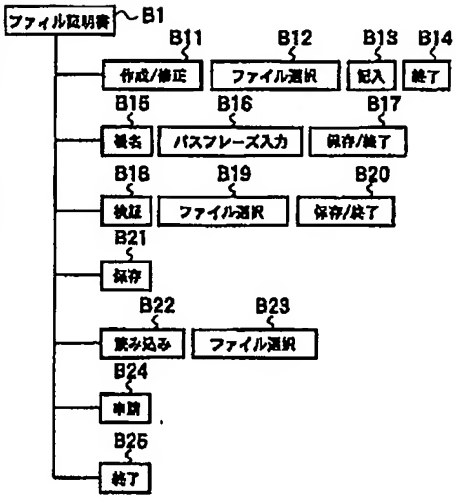
【図９】


開始
外部転送メールを受信
S11
メール中から宛先情報を読み出し
S13
転送制御テーブルから宛先情報に対応する
転送条件、資料区分、転送処理削除、転送
不可通知の各情報を読み出し
S15
S17
メール情報が転送条件情報
を満足するか?
NO
YES
S19
メール情報が資料区分情報
を満足するか?
NO
YES
S21
配布リスト、ファイル証明書
を削除するか?
NO
YES
削除
S23
メール送信
S25
送信不可通知
S27
終了

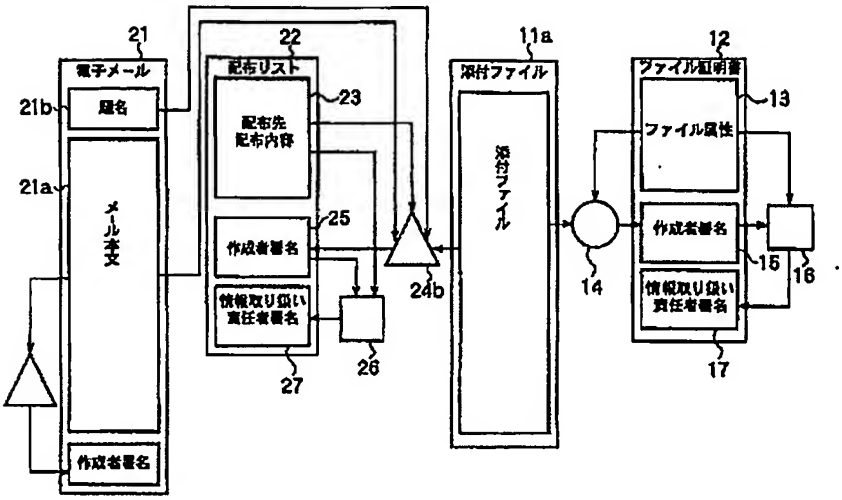
【図６】


21
電子メール
署名
21b
21a
メール本文
作成者署名
22
配布リスト
配布先
配布内容
23
作成者署名
25
情報取り扱い
責任者署名
ハッシュ値
の結合
24ハッシュ
値の結合
26
27
11a
添付ファイル

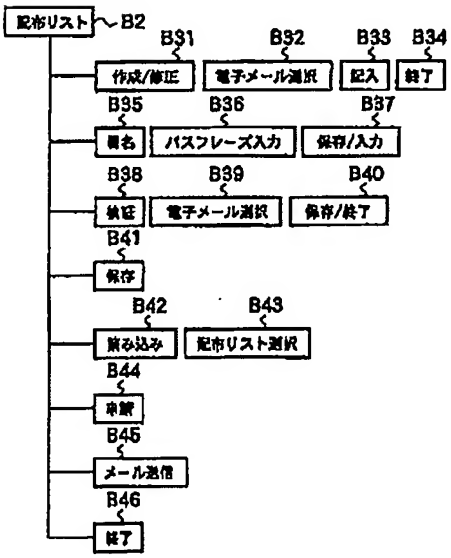
【図１１】


ファイル証明書
B1
B11
作成/修正
B12
ファイル選択
B13
記入
B14
終了
B15
署名
B16
パスフレーズ入力
B17
保存/終了
B18
検証
B19
ファイル選択
B20
保存/終了
B21
保存
B22
読み込み
B23
ファイル選択
B24
申請
B25
終了

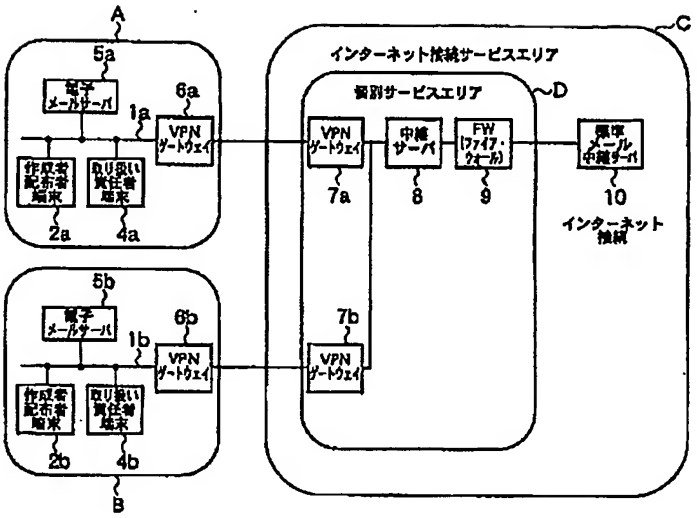
【図７】


21
22
11a
12
電子メール
配布リスト
添付ファイル
ファイル証明書
21b
題名
23
配布先
配布内容
13
ファイル属性
21a
メール本文
25
作成者署名
作成者署名
15
16
情報取り扱い
責任者署名
24b
14
情報取り扱い
責任者署名
27
26
17
作成者署名

【図１２】


配布リスト
B2
B31
B32
B33
B34
作成/修正
電子メール選択
記入
終了
B35
B36
B37
署名
パスフレーズ入力
保存/入力
B38
B39
B40
検証
電子メール選択
保存/終了
B41
保存
B42
B43
読み込み
配布リスト選択
B44
中断
B45
メール送信
B46
終了

【図１３】


A
5a
電子メールサーバ
6a
1a
VPN ゲートウェイ
作成者記述者端末
取り扱い責任者端末
2a
4a
5b
電子メールサーバ
6b
1b
VPN ゲートウェイ
作成者記述者端末
取り扱い責任者端末
2b
4b
B
C
インターネット接続サービスエリア
個別サービスエリア
D
VPN ゲートウェイ
7a
中継サーバ
8
FW (ファイア・ウォール)
9
標準メール中継サーバ
10
インターネット接続
VPN ゲートウェイ
7b

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-232487

(43)Date of publication of application : 16.08.2002

(51)Int.Cl. H04L 12/58
G06F 13/00
G09C 1/00
H04L 12/66

(21)Application number : 2001-025758

(22)Date of filing : 01.02.2001

(71)Applicant : TOSHIBA CORP

(72)Inventor : TAKAHASHI YOICHI

(54) ELECTRONIC MAIL SYSTEM AND ELECTRONIC MAIL TRANSMISSION CONTROL METHOD, AND REPEATER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic mail system that secures the security of transmission of electronic mail by a certificate and a signature and changes the security of decision of the certificate so as to select ease of use or a degree of the security depending on the policy.

SOLUTION: An electronic mail server 5 receives electronic mail from terminals 2, 3, 4, a relay server 6 receives electronic mail from the electronic mail server, transmission of the electronic mail to an external domain is inhibited as the fundamental settings and the transmission of the electronic mail to the external domain is permitted when a specific condition is established. Furthermore, the terminal generates a file certificate to certify contents of an attached file in the case of generating the attached file, signs the file certificate to warrant the relation between the attached file and the file certificate and the contents of the attached file, and the relay server decides the propriety of transmission of the electronic mail to the external domain on the basis of the file certificate and the contents of the signature attached to the attached file sent from the terminal and transmits only the electronic mail with the permitted contents to the external domain.